

(19)



JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **2001077802 A**

(43) Date of publication of application: **23.03.01**

(51) Int. Cl.  
**H04L 9/08**  
**G06F 12/14**  
**G11B 20/10**  
**H04N 5/84**  
**H04N 5/91**

(21) Application number: **11248420**

(22) Date of filing: **02.09.99**

(71) Applicant: **SONY CORP**

(72) Inventor:  
**OSAWA YOSHITOMO**  
**ASANO TOMOYUKI**

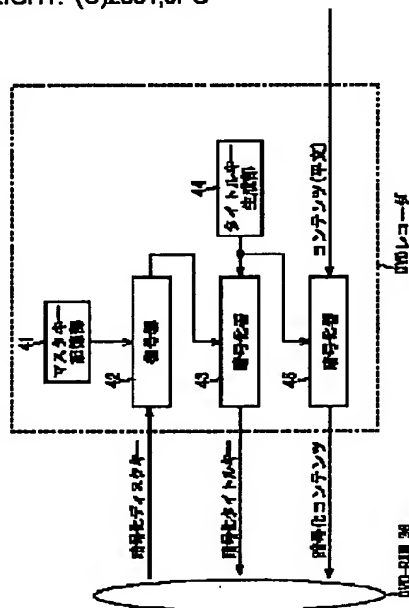
(54) **DATA PROVIDING DEVICE, DATA PROVIDING METHOD, PROGRAM RECORDING MEDIUM, DATA RECORDING MEDIUM AND MANUFACTURE OF DATA RECORDING MEDIUM**

COPYRIGHT: (C)2001,JPO

(57) Abstract

**PROBLEM TO BE SOLVED:** To prevent an illegal copy to a DVD-RAM and to reproduce the DVD-RAM to which the legal copy is made by using an existing DVD player.

**SOLUTION:** A disk key encrypted by a master key (encrypted disk key) is stored in advance in a DVD-RAM 36, a decoder 42 reads the encrypted disk key from the DVD-RAM 36 and decodes it by using the master key stored in a master key storage section 41. Furthermore, an encryption device 43 encrypts the title key outputted from a title key generating section 44 by using the master key decoded by the decoder 42 and stores the encrypted title key obtained as a result to the DVD-RAM 36. Then an encryption device 45 encrypts contents by using the title key outputted from the title key generating section 44 and stores it to the DVD-RAM 36.



(19)日本国特許庁(JP)

## (12) 公開特許公報 (A)

(11)特許出願公開番号

特開2001-77802

(P2001-77802A)

(43)公開日 平成13年3月23日(2001.3.23)

(51)Int.Cl. <sup>7</sup>	識別記号	F I	テ-マ-コ-ト <sup>7</sup> (参考)	
H 0 4 L 9/08		H 0 4 L 9/00	6 0 1 A	5 B 0 1 7
G 0 6 F 12/14	3 2 0	G 0 6 F 12/14	3 2 0 B	5 C 0 5 2
			3 2 0 E	5 C 0 5 3
G 1 1 B 20/10		G 1 1 B 20/10	H	5 D 0 4 4
H 0 4 N 5/84		H 0 4 N 5/84	Z	5 J 1 0 4

審査請求 未請求 請求項の数16 OL (全 19 頁) 最終頁に続く

(21)出願番号 特願平11-248420

(22)出願日 平成11年9月2日(1999.9.2)

(71)出願人 000002185

ソニー株式会社

東京都品川区北品川6丁目7番35号

(72)発明者 大澤 義知

東京都品川区北品川6丁目7番35号 ソニ

ー株式会社内

(72)発明者 浅野 智之

東京都品川区北品川6丁目7番35号 ソニ

ー株式会社内

(74)代理人 100082131

弁理士 稲本 義雄

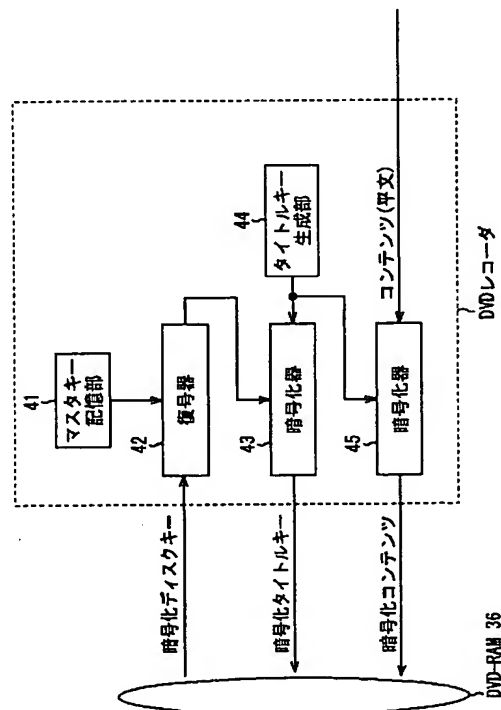
最終頁に続く

(54)【発明の名称】 データ提供装置、データ提供方法、およびプログラム記録媒体、並びにデータ記録媒体、およびデータ記録媒体の製造方法

## (57)【要約】

【課題】 DVD-RAMに対する違法コピーを防止するとともに、適法なコピーが行われたDVD-RAMを、現行のDVDプレーヤで再生する。

【解決手段】 DVD-RAM36には、マスターキーで暗号化されたディスクキー（暗号化ディスクキー）があらかじめ記録されており、復号器42は、暗号化ディスクキーを、DVD-RAM36から読み出し、マスターキー記憶部41に記憶されているマスターキーで復号する。さらに、暗号化器43は、タイトルキー生成部44が出力するタイトルキーを、復号器42が復号したマスターキーで暗号化し、その結果得られる暗号化タイトルキーを、DVD-RAM36に記録する。そして、暗号化器45は、コンテンツを、タイトルキー生成部44が出力するタイトルキーで暗号化し、DVD-RAM36に記録する。



## 【特許請求の範囲】

【請求項 1】 データを暗号化して提供するデータ提供装置であって、

第 1 キーで暗号化された第 2 キーである暗号化第 2 キーを取得する取得手段と、

前記暗号化第 2 キーを、前記第 1 キーに基づいて復号する暗号化第 2 キー復号手段と、

前記暗号化第 2 キー復号手段により復号された前記第 2 キーを利用して、前記データを暗号化する暗号化手段と、

前記暗号化手段により暗号化された前記データである暗号化データを提供する提供手段とを含むことを特徴とするデータ提供装置。

【請求項 2】 前記暗号化手段は、

第 3 キーを、前記第 2 キーで暗号化し、暗号化第 3 キーを出力する第 3 キー暗号化手段と、

前記データを、前記第 3 キーで暗号化するデータ暗号化手段とを有し、

前記提供手段は、前記暗号化データを、前記暗号化第 3 キーとともに提供することを特徴とする請求項 1 に記載のデータ提供装置。

【請求項 3】 前記第 1 キーを記憶している記憶手段をさらに含むことを特徴とする請求項 1 に記載のデータ提供装置。

【請求項 4】 前記取得手段は、複数の第 1 キーそれぞれで暗号化された第 2 キーである暗号化第 2 キーのセットのうち、前記記憶手段に記憶されている前記第 1 キーで復号可能なものを取得することを特徴とする請求項 3 に記載のデータ提供装置。

【請求項 5】 前記暗号化第 2 キー復号手段による復号方法、および前記暗号化手段による暗号化方法は、DVD (Digital Versatile Disc) 規格に準拠したものであることを特徴とする請求項 1 に記載のデータ提供装置。

【請求項 6】 前記取得手段は、データ記録媒体に記録された前記暗号化第 2 キーを読み出すことを特徴とする請求項 1 に記載のデータ提供装置。

【請求項 7】 前記取得手段は、伝送路を介して伝送されてくる前記暗号化第 2 キーを受信することを特徴とする請求項 1 に記載のデータ提供装置。

【請求項 8】 前記提供手段は、前記暗号化データを、データ記録媒体に記録することを特徴とする請求項 1 に記載のデータ提供装置。

【請求項 9】 前記提供手段は、前記暗号化データを、伝送路を介して伝送することを特徴とする請求項 1 に記載のデータ提供装置。

【請求項 10】 データを暗号化して提供するデータ提供方法であって、

第 1 キーで暗号化された第 2 キーである暗号化第 2 キーを取得する取得ステップと、

前記暗号化第 2 キーを、前記第 1 キーに基づいて復号す

る暗号化第 2 キー復号ステップと、

前記暗号化第 2 キー復号ステップにおいて復号された前記第 2 キーを利用して、前記データを暗号化する暗号化ステップと、

前記暗号化ステップにおいて暗号化された前記データである暗号化データを提供する提供ステップとを含むことを特徴とするデータ提供方法。

【請求項 11】 データを暗号化して提供するデータ提供処理を、コンピュータに行わせるためのプログラムが記録されているプログラム記録媒体であって、

第 1 キーで暗号化された第 2 キーである暗号化第 2 キーを取得する取得ステップと、

前記暗号化第 2 キーを、前記第 1 キーに基づいて復号する暗号化第 2 キー復号ステップと、

前記暗号化第 2 キー復号ステップにおいて復号された前記第 2 キーを利用して、前記データを暗号化する暗号化ステップと、

前記暗号化ステップにおいて暗号化された前記データである暗号化データを提供する提供ステップとを含むプログラムが記録されていることを特徴とするプログラム記録媒体。

【請求項 12】 データが暗号化されて記録される記録可能なデータ記録媒体であって、

第 1 キーで暗号化された第 2 キーである暗号化第 2 キーが記録されており、

後に、前記暗号化第 2 キーを、前記第 1 キーで復号し、前記第 2 キーを得て、その第 2 キーを利用して、前記データが暗号化されて記録されることを特徴とするデータ記録媒体。

【請求項 13】 DVD (Digital Versatile Disc) 規格に準拠したフォーマットを有することを特徴とする請求項 12 に記載のデータ記録媒体。

【請求項 14】 複数の第 1 キーそれぞれで暗号化された第 2 キーである暗号化第 2 キーのセットが記録されていることを特徴とする請求項 12 に記載のデータ記録媒体。

【請求項 15】 前記暗号化第 2 キーは、読み出しが可能であるが、書き込みが不可能な記録領域に記録されていることを特徴とする請求項 12 に記載のデータ記録媒体。

【請求項 16】 データが暗号化されて記録される記録可能なデータ記録媒体の製造方法であって、

後に、第 1 キーで暗号化された第 2 キーである暗号化第 2 キーを、前記第 1 キーで復号し、前記第 2 キーを得て、その第 2 キーを利用して、前記データが暗号化されて記録されるデータ記録媒体に、前記暗号化第 2 キーを記録することを特徴とするデータ記録媒体の製造方法。

## 【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、データ提供装置、

データ提供方法、およびプログラム記録媒体、並びにデータ記録媒体、およびデータ記録媒体の製造方法に関し、特に、例えば、DVD-RAM(Digital Versatile Disc - Random Access Memory)に対する違法コピーを防止するとともに、適法なコピーが行われたDVD-RAMを、現行のDVDプレーヤで再生することができるようにするデータ提供装置、データ提供方法、およびプログラム記録媒体、並びにデータ記録媒体、およびデータ記録媒体の製造方法に関する。

#### 【0002】

【従来の技術】デジタル信号処理技術の進歩、発展に伴い、近年においては、情報を、デジタル的に記録する記録装置や記録媒体が普及しつつある。

【0003】このような記録装置および記録媒体によれば、例えば、画像や音声を劣化させることなく記録を繰り返すことができるため、即ち、画質や音質を維持したまま、何度もコピーすることができるため、そのようなコピーが違法に行われた記録媒体が、市場に流通すれば、映画等の著作権者等の利益が害されることになる。そこで、記録装置および記録媒体には、違法なコピーを行うことができないような仕組み(システム)が導入されている。

【0004】即ち、例えば、ミニディスク装置においては(ミニディスクは商標)、違法なコピーを防止する方法として、SCMS(Serial Copy Management System)が採用されている。SCMSは、再生側において、オーディオデータとともに、SCMS信号を、デジタルインタフェース(DIF)から出力し、記録側において、再生側からのSCMS信号に基づいて、同じく再生側からのオーディオデータの記録を制御することにより、違法なコピーを防止するようになっている。

【0005】即ち、SCMS信号は、オーディオデータが、コピーフリーのもの(copy free)であるか、1度だけコピーが許されているもの(copy once allowed)であるか、またはコピーが禁止されているもの(copy prohibited)であるかを表す信号で、記録側では、DIFからオーディオデータを受信すると、そのオーディオデータとともに送信されてくるSCMS信号を検出する。そして、SCMS信号が、copy freeとなっている場合には、オーディオデータを、SCMS信号とともに、ミニディスクに記録する。また、SCMS信号が、copy once allowedとなっている場合には、SCMS信号を、copy prohibitedに変更して、オーディオデータとともに、ミニディスクに記録し、SCMS信号が、copy prohibitedとなっている場合には、オーディオデータの記録を行わない。

【0006】以上のようにして、ミニディスク装置では、SCMSによって、著作権を有するオーディオデータが、違法にコピーされるのを防止するようになっている。

【0007】しかしながら、SCMSでは、上述のように、SCMS信号に基づいて、再生側からのオーディオデータの記録を制御するようにはなっていないミニディスク装置が製造された場合に対処するのが困難である。

【0008】そこで、例えば、DVDプレーヤでは、コンテンツスクランブルシステムを採用することにより、著作権を有するデータが、違法にコピーされるのを防止するようになっている。

【0009】コンテンツスクランブルシステムでは、DVD-ROM(Read Only Memory)に、ビデオデータやオーディオデータ等が暗号化されて記録されており、その暗号化されたデータを復号するのに用いるキーが、ライセンスを受けたDVDプレーヤに与えられる。ライセンスは、DVDプレーヤを、不正コピーを行わない等の所定の動作規定にしたがうように設計することを条件に与えられ、従って、ライセンスを受けたDVDプレーヤでは、与えられたキーを利用して、暗号化されたデータを復号することにより、DVD-ROMに記録された画像や音声を再生することができる。一方、ライセンスを受けていないDVDプレーヤは、暗号化されたデータを復号するためのキーを有していないため、その復号を行うことができず、これにより、ライセンス時に要求される条件を満たしていないDVDプレーヤによって、DVD-ROMが再生されることによる、不正なコピーが防止されるようになっている。

【0010】コンテンツスクランブルシステムで採用されているDVD-ROMは、図1に示すように製造される。

【0011】即ち、コンテンツ供給者である、映画会社その他の著作権者等は、ディスクキーとタイトルキーと呼ばれる、DVD-ROMに記録される映画等のコンテンツの暗号化および復号に利用される2つのキーを決定して発行する。

【0012】鍵管理センタ4は、DVDプレーヤの製造に用いられるLSI(Large Scale Integrated Circuit)やソフトウェアモジュールのメーカに割り当てる複数のマスタキーを設定し、暗号化器5において、その複数のマスタキーそれぞれで、ディスクキーを暗号化することにより、暗号化されたディスクキー(以下、適宜、暗号化ディスクキーという)のセットを作成する。さらに、暗号化器6において、ディスクキーで、タイトルキーが暗号化され、暗号化されたタイトルキー(以下、適宜、暗号化タイトルキーという)が作成される。そして、鍵管理センタ4は、暗号化ディスクキーのセットと、暗号化タイトルキーを、DVD-ROMの製造業者であるディスク製造業者7に提供する。

【0013】ディスク製造業者7では、圧縮器2において、データベース1に登録されている画像や音声等のデジタルデータであるコンテンツが、例えば、MPEG(Moving Picture Experts Group)2方式によって圧縮さ

れ、暗号化器3において、圧縮器2が出力するコンテンツが、コンテンツ供給者が発行するタイトルキーで暗号化され、暗号化コンテンツとされる。

【0014】さらに、ディスク製造業者7では、暗号化コンテンツとともに、鍵管理センタ4から提供される暗号化ディスクキーのセットと暗号化タイトルキーが記録されたDVD-ROMの原盤（ディスク原盤）8が作成され、その原盤8を用いて、スタンパ9が作成される。そして、そのスタンパ9を用いて、多数のDVD-ROM10が製造される。

【0015】なお、鍵発行センタ4とディスク製造業者7とは、異なる組織であっても、同一の組織であってもかまわない。また、図1では、ディスク製造業者7において、コンテンツを暗号化するようにしたが、コンテンツの暗号化も、鍵管理センタ4で行い、鍵管理センタ4から、ディスク製造業者7には、暗号化ディスクキーのセットおよび暗号化タイトルキーとともに、暗号化コンテンツを提供するようにすることが可能である。

【0016】図2は、以上のようにして製造されるDVD-ROM10について、DVD規格で規定されているディスクフォーマットを示している。

【0017】図2（A）に示すように、物理セクタ番号が0h（hは、その前の数字が16進数であることを表す）の物理セクタ（物理セクタ番号がxの物理セクタを、以下、適宜、物理セクタ#xと記述する）から、物理セクタ#2FFFFhまでは、リードイン領域となっており、物理セクタ#30000h以降が、コンテンツが記録されるメインデータ領域となっている。

【0018】リードイン領域は、物理セクタ#0hから#2EFFFhまでが0の領域に、物理セクタ#2F000hから#2F01Fhまでが参照用コードの領域に、物理セクタ#2F020hから#2F1FFFhまでが0の領域に、物理セクタ#2F200hから#2FDFFFhまでがコントロールデータ領域に、物理セクタ#2FE00hから#2FFFFhまでが0の領域に、それぞれなっており、暗号化ディスクキーのセットは、コントロールデータ領域に記録される。

【0019】即ち、コントロールデータ領域の先頭の物理セクタは、ディスク構造等の物理フォーマット情報が記録される領域に、2番目の物理セクタは、ディスク製造情報が記録される領域に、3番目から16番目までの物理セクタは、コンテンツ供給者の情報が記録される領域に、それぞれなっており、それ以降のコントロールデータ領域は、その先頭から16番目までの物理セクタと同様の領域が繰り返されるようになっている。そして、暗号化ディスクキーのセットは、以上のようなコントロールデータ領域のうちの、コンテンツ供給者の情報が記録される領域に記録される。

【0020】メインデータ領域には、図2（B）に示すような2064バイト単位の論理セクタであるデータセ

クタが繰り返し配置されており、データセクタは、セクタ番号等のID(Identification)が配置される領域、IDの誤り検出用データが配置される領域、コピー管理用データが配置される領域、ユーザデータが配置される領域、データセクタ全体の誤り検出用データが配置される領域から構成される。暗号化タイトルキーは、以上のようなデータセクタのうちの、コピー管理用データが配置される領域に記録される。

【0021】なお、暗号化ディスクキーのセットが記録される領域、および暗号化タイトルキーが記録される領域は、いずれも、コンピュータの論理ファイルシステムを介して読み出せないようになっており、これにより、ディスクキーやタイトルキーが、DVDプレーヤの外部に漏れることを防止するようになっている。但し、暗号化ディスクキーのセットが記録される領域、および暗号化タイトルキーが記録される領域は、あくまでも、コンピュータの論理ファイルシステムを介して読み出せないだけで、DVDプレーヤの内部では、暗号化ディスクキーや暗号化タイトルキーが読み出され、暗号化タイトルキーや暗号化コンテンツの復号に用いられる。

【0022】次に、図3は、図2に示したフォーマットのDVD-ROM10の再生を行う、従来（現行）のDVDプレーヤの一例の構成を示している。

【0023】ライセンスを受けたDVDプレーヤは、そのDVDプレーヤのメーカーに割り当てられたマスタキー（以下、適宜、割り当てマスタキーという）を記憶しているマスタキー記憶部21を有しており、復号器22は、DVD-ROM10に記録された暗号化ディスクキーのセットの中から、その割り当てマスタキーで暗号化されているものを読み出す。

【0024】ここで、DVD-ROM10に記録された暗号化ディスクキーのセットのうち、何番目のディスクキー（暗号化ディスクキー）が、DVDプレーヤのメーカーに割り当てられているかに関する情報は、そのメーカーに対して、ライセンス契約時に、マスタキーとともに与えられるようになっており、DVDプレーヤでは、その情報に基づいて、自身の割り当てマスタキーで暗号化されている暗号化ディスクキーが、DVD-ROM10から読み出されるようになっている。

【0025】復号器22は、マスタキー記憶部21に記憶されている割り当てマスタキーを読み出し、DVD-ROM10から読み出した暗号化ディスクキーを、割り当てマスタキーで復号する。そして、復号器22は、その復号の結果得られるディスクキーを、復号器23に供給する。

【0026】復号器23は、DVD-ROM10におけるデータセクタのコピー管理用データ領域に記録されている暗号化タイトルキーを読み出し、その暗号化タイトルキーを、復号器22からのディスクキーで復号する。そして、復号器23は、その復号の結果得られるタイト

ルキーを、復号器24に供給する。

【0027】復号器24は、DVD-ROM10におけるデータセクタのユーザデータ領域に記録されている暗号化コンテンツを読み出し、その暗号化コンテンツを、復号器23からのタイトルキーで復号する。復号器24による復号の結果得られるデジタルデータのコンテンツ（いわゆる平文とされたコンテンツ）は、A/D(Analog/Digital)変換され、アナログ信号とされて、外部に出力される。

【0028】なお、上述したコンテンツスクランブルシステムについては、例えば、「日経エレクトロニクス」、1997年8月18日（no. 696）、pp. 110-119、日経BP社等に、その詳細が記載されている。

#### 【0029】

【発明が解決しようとする課題】以上のような、DVD-ROMで採用されているコンテンツスクランブルシステムは、ユーザによるデータの書き込みが不可能な記録媒体（以下、適宜、ROMメディアという）を対象としており、ユーザによるデータの書き込みが可能な記録媒体（以下、適宜、RAMメディアという）への適用については考慮されていない。

【0030】即ち、RAMメディアである、例えば、DVD-RAMに、コンテンツスクランブルシステムを採用するには、そのDVD-RAMに記録するコンテンツのコンテンツ供給者によって発行されるタイトルキーやディスクキーが必要となるが、将来、どのようなコンテンツが記録されるか分からないDVD-RAMについて、コンテンツ供給者が、タイトルキーやディスクキーを発行するのは困難である（コンテンツ供給者が、どのようなコンテンツが記録されるか分からないDVD-RAMに対して、タイトルキーやディスクキーを決めることはできない）。

【0031】そこで、DVD-RAM等のRAMメディアについては、コンテンツスクランブルシステムとは異なる方法で、違法コピーを防止するようにすることも可能であるが、この場合、そのような異なる方法が採用したDVD-RAMを、現行のDVDプレーヤで再生することはできなくなる。従って、コンテンツスクランブルシステムとは異なる方法をDVD-RAMに採用した場合には、そのようなDVD-RAMに対応したDVDプレーヤを、現行のDVDプレーヤを有するユーザに新たに購入してもらわなければならないため、コンテンツスクランブルシステムとは異なる方法を、RAMメディアに採用するのは好ましくない。

【0032】本発明は、このような状況に鑑みてなされたものであり、RAMメディアに対する違法コピーを防止するとともに、適法なコピーが行われたRAMメディアを、現行のプレーヤで再生することができるようにするものである。

#### 【0033】

【課題を解決するための手段】本発明のデータ提供装置は、第1キーで暗号化された第2キーである暗号化第2キーを取得する取得手段と、暗号化第2キーを、第1キーに基づいて復号する暗号化第2キー復号手段と、暗号化第2キー復号手段により復号された第2キーを利用して、データを暗号化する暗号化手段と、暗号化手段により暗号化されたデータである暗号化データを提供する提供手段とを含むことを特徴とする。

【0034】暗号化手段には、第3キーを、第2キーで暗号化し、暗号化第3キーを出力する第3キー暗号化手段と、データを、第3キーで暗号化するデータ暗号化手段とを設けることができ、この場合、提供手段には、暗号化データを、暗号化第3キーとともに提供させることができる。

【0035】データ提供装置には、第1キーを記憶している記憶手段をさらに設けることができる。

【0036】取得手段には、複数の第1キーそれぞれで暗号化された第2キーである暗号化第2キーのセットのうち、記憶手段に記憶されている第1キーで復号可能なものを取得させることができる。

【0037】暗号化第2キー復号手段による復号方法、および暗号化手段による暗号化方法は、DVD(Digital Versatile Disc)規格に準拠したものとすることができる。

【0038】取得手段には、データ記録媒体に記録された暗号化第2キーを読み出させることができる。また、取得手段には、伝送路を介して伝送されてくる暗号化第2キーを受信させることができる。

【0039】提供手段には、暗号化データを、データ記録媒体に記録させることができる。また、提供手段には、暗号化データを、伝送路を介して伝送させることができる。

【0040】本発明のデータ提供方法は、第1キーで暗号化された第2キーである暗号化第2キーを取得する取得ステップと、暗号化第2キーを、第1キーに基づいて復号する暗号化第2キー復号ステップと、暗号化第2キー復号ステップにおいて復号された第2キーを利用して、データを暗号化する暗号化ステップと、暗号化ステップにおいて暗号化されたデータである暗号化データを提供する提供ステップとを含むことを特徴とする。

【0041】本発明のプログラム記録媒体は、第1キーで暗号化された第2キーである暗号化第2キーを取得する取得ステップと、暗号化第2キーを、第1キーに基づいて復号する暗号化第2キー復号ステップと、暗号化第2キー復号ステップにおいて復号された第2キーを利用して、データを暗号化する暗号化ステップと、暗号化ステップにおいて暗号化されたデータである暗号化データを提供する提供ステップとを含むプログラムが記録されていることを特徴とする。

【0042】本発明のデータ記録媒体は、第1キーで暗号化された第2キーである暗号化第2キーが記録されており、後に、暗号化第2キーを、第1キーで復号し、第2キーを得て、その第2キーを利用して、データが暗号化されて記録されることを特徴とする。

【0043】このデータ記録媒体は、DVD(Digital Versatile Disc)規格に準拠したフォーマットを有するものとすることができる。

【0044】また、このデータ記録媒体は、複数の第1キーそれぞれで暗号化された第2キーである暗号化第2キーのセットが記録されているものとすることができる。

【0045】暗号化第2キーは、読み出しが可能であるが、書き込みが不可能な記録領域に記録しておくようにすることができる。

【0046】本発明のデータ記録媒体の製造方法は、後に、第1キーで暗号化された第2キーである暗号化第2キーを、第1キーで復号し、第2キーを得て、その第2キーを利用して、データが暗号化されて記録されるデータ記録媒体に、暗号化第2キーを記録することを特徴とする。

【0047】本発明のデータ提供装置およびデータ提供方法、並びにプログラム記録媒体においては、第1キーで暗号化された第2キーである暗号化第2キーが取得され、暗号化第2キーが、第1キーに基づいて復号される。そして、その復号された第2キーを利用して、データが暗号化され、その暗号化されたデータである暗号化データが提供される。

【0048】本発明のデータ記録媒体においては、第1キーで暗号化された第2キーである暗号化第2キーが記録されており、後に、暗号化第2キーが、第1キーで復号され、その結果得られる第2キーを利用して、データが暗号化されて記録される。

【0049】本発明のデータ記録媒体の製造方法においては、後に、第1キーで暗号化された第2キーである暗号化第2キーを、第1キーで復号し、第2キーを得て、その第2キーを利用して、データが暗号化されて記録されるデータ記録媒体に、暗号化第2キーが記録される。

#### 【0050】

【発明の実施の形態】図4は、本発明を適用したRAMメディアであるDVD-RAMの製造工程の一実施の形態を示している。

【0051】DVD-RAMの製造は、図4に示すように、鍵管理センタ31およびディスク製造業者33によって行われる。

【0052】即ち、鍵管理センタ31では、図5のフローチャートに示すように、まず最初に、ステップS1において、DVD-RAMに用いる適当なディスクキー(第2キー)が決定され、ステップS2に進み、図1の鍵管理センタ4における場合と同様に、DVD規格に準

拠した暗号化を行う暗号化器32によって、ディスクキーを、複数のマスタキー(第1キー)それぞれで暗号化することにより、暗号化ディスクキーのセットが作成される。鍵管理センタ31で作成された暗号化ディスクキーのセットは、ステップ3において、ディスク製造業者33に提供される。

【0053】なお、鍵管理センタ31は、ライセンス契約を行ったメーカそれぞれに対して、異なるマスタキーを割り当てる。鍵管理センタ31は、ディスクキーの暗号化に用いる複数のマスタキーとして、十分な数のマスタキーを用意しており(従って、ディスクキーは、そのような十分な数のマスタキーそれぞれで暗号化される)、これにより、ライセンス契約を行うメーカの数が増加しても、各メーカに、異なるマスタキーを割り当てることができるようになっている。

【0054】ディスク製造業者33では、図6のフローチャートに示すように、まず最初に、ステップS11において、鍵管理センタ31から提供される暗号化ディスクキーのセットが取得され、ステップS12に進み、その暗号化ディスクキーのセットが記録された、DVD規格に準拠したフォーマットのDVD-RAMの原盤(ディスク原盤)34が作成される。即ち、ディスク製造業者33においては、ステップS12において、前述の図2に示したようなフォーマットを有するDVD-RAMの原盤34であって、そのリードイン領域のコントロールデータ領域に、暗号化ディスクキーのセットが記録されたものが作成される。さらに、ディスク製造業者33では、ステップS13において、原盤34を用いて、スタンパ35が作成され、ステップS14に進み、そのスタンパ35を用いて、多数のDVD-RAM36が製造(スタンプ)される。

【0055】以上のようにして、図2に示したDVD規格に規定されているフォーマットのDVD-RAM36が製造される。

【0056】なお、DVD-RAM36は、上述のように、スタンパ35を用いてスタンプが行われることにより製造されるから、暗号化ディスクキーのセットが記録される記録領域(リードイン領域のコントロールデータ領域(図2(A)))は、読み出しは可能であるが、書き込みが不可能な領域となる。

【0057】ここで、違法コピーを、より強固に防止するため、鍵管理センタ31においては、ディスクキーを頻繁に更新するようにし、できるだけ、異なるディスクキー(暗号化ディスクキー)が記録されたDVD-RAMが製造されるようにするのが望ましい。

【0058】また、鍵発行センタ31とディスク製造業者33とは、異なる組織であっても、同一の組織であってもかまわない。

【0059】次に、図7は、図4乃至図6で説明したようにして製造されたDVD-RAM36に対して、ディ



デジタルデータのコンテンツを記録するDVDレコーダの一実施の形態の構成例を示している。

【0060】マスタキー記憶部41は、DVDレコーダ(のLSIやソフトウェアモジュール)のメーカに割り当てられたマスタキー(割り当てマスタキー)を記憶している。

【0061】復号器42は、DVD-RAM36のリードイン領域に記録された暗号化ディスクキーのセットの中から、割り当てマスタキーで暗号化されたものを読み出し(取得し)、マスタキー記憶部41に記憶されているマスタキーで、DVD規格に準拠した復号方法(復号アルゴリズム)により復号するようになっている。復号器42による復号の結果得られるディスクキーは、暗号化器43に供給されるようになっている。

【0062】暗号化器43は、タイトルキー生成部44から供給されるタイトルキーを、復号器42から供給されるディスクキーで、DVD規格に準拠した暗号化方法(暗号化アルゴリズム)により暗号化し、その結果得られる暗号化タイトルキーを、DVD-RAM36におけるデータセクタ(図2(B))のコピー管理用データ領域に記録(提供)するようになっている。

【0063】タイトルキー生成部44は、タイトルキー(第3キー)として用いることのできるキーを、例えば、乱数等を利用して生成し、暗号化器43および45に供給するようになっている。

【0064】暗号化器45は、DVD-RAM36に記録しようとするコンテンツとしてのデジタルデータを受信し、そのコンテンツを、タイトルキー生成部44から供給されるタイトルキーで、DVD規格に準拠した暗号化方法により暗号化するようになっている。さらに、暗号化器45は、その暗号化の結果得られる暗号化コンテンツを、DVD-RAM36におけるデータセクタのユーザデータ領域に記録するようになっている。

【0065】以上のように構成されるDVDレコーダでは、図8のフローチャートに示すようにして、DVD-RAM36へのコンテンツの記録が行われる。

【0066】即ち、まず最初に、ステップS21において、復号器42は、DVD-RAM36のリードイン領域に記録された暗号化ディスクキーのセットの中から、割り当てマスタキーで暗号化されたものを読み出し、ステップS22に進み、マスタキー記憶部41に記憶されているマスタキーで復号して、ディスクキーを得る。このディスクキーは、復号部42から暗号化器43に供給される。

【0067】そして、ステップS23に進み、タイトルキー生成部44において、タイトルキーが生成され、暗号化器43および45に供給される。暗号化器43は、ステップS24において、タイトルキー生成部44から供給されるタイトルキーを、復号器42から供給されるディスクキーで暗号化し、その結果得られる暗号化タイ

トルキーを、DVD-RAM36に記録する。

【0068】その後、DVD-RAM36に記録すべきコンテンツが、暗号化器45に入力されると、暗号化器45は、ステップS25において、そのコンテンツを受信し、ステップS26に進み、そのコンテンツを、タイトルキー生成部44からのタイトルキーで暗号化し、DVD-RAM36に記録する。そして、ステップS27に進み、記録対象のコンテンツを、すべて記録したかどうか判定され、まだ記録していないと判定された場合、暗号化器45に、次のコンテンツが入力されるのを待って、ステップS25に戻り、以下、同様の処理を繰り返す。

【0069】また、ステップS27において、記録対象のコンテンツを、すべて記録したと判定された場合、処理を終了する。

【0070】以上のようにして、コンテンツが記録されたDVD-RAM36には、図1で説明したようにして製造されるDVD-ROM10と同一フォーマットで、暗号化ディスクキーのセット、暗号化タイトルキー、および暗号化コンテンツが記録されている。従って、DVD-RAM36は、マスタキーを有していないDVDプレーヤでは再生することができないので、不正なコピーを防止することができ、さらに、DVD-ROM10を再生する図3のDVDプレーヤと同一のDVDプレーヤで再生することができる。即ち、DVD-RAMに対する違法コピーを防止するとともに、適法なコピーが行われたDVD-RAMを、現行のDVDプレーヤで再生することができる。

【0071】次に、図9は、DVD-RAM36を再生するDVDプレーヤの構成例を示している。

【0072】図9におけるマスタキー記憶部51、または復号器52乃至54は、図3におけるマスタキー記憶部21、または復号器22乃至24とそれぞれ同様に構成されており、従って、図9のDVDプレーヤでは、図3におけるDVDプレーヤがDVD-ROM10を再生するのと同様にして、DVD-RAM36が再生される。

【0073】即ち、図9のDVDプレーヤでは、図10のフローチャートに示すように、まず最初に、ステップS31において、復号器52は、DVD-RAM36のリードイン領域に記録された暗号化ディスクキーのセットの中から、マスタキー記憶部51に記憶されている割り当てマスタキーで暗号化されているものを読み出す。さらに、復号器52は、ステップS32において、マスタキー記憶部51に記憶されている割り当てマスタキーを読み出し、DVD-RAM36から読み出した暗号化ディスクキーを、割り当てマスタキーで復号する。そして、復号器52は、その復号の結果得られるディスクキーを、復号器53に供給する。

【0074】復号器53は、ステップS33において、



DVD-RAM36におけるデータセクタのコピー管理用データ領域に記録されている暗号化タイトルキーを読み出し、ステップS34に進み、その暗号化タイトルキーを、復号器52からのディスクキーで復号する。そして、復号器53は、その復号の結果得られるタイトルキーを、復号器54に供給する。

【0075】復号器54は、ステップS35において、DVD-RAM36におけるデータセクタのユーザデータ領域に記録されている暗号化コンテンツを読み出し、ステップS36に進み、その暗号化コンテンツを、復号器53からのタイトルキーで復号する。復号器54による復号の結果得られるデジタルデータのコンテンツ（いわゆる平文とされたコンテンツ）は、A/D(Analog/Digital)変換され、アナログ信号とされて、外部に出力される。

【0076】そして、ステップS37に進み、再生対象のコンテンツを、すべて再生したかどうか判定され、まだ再生していないと判定された場合、ステップS35に戻り、次に再生すべき暗号化コンテンツを、DVD-RAM36から読み出し、以下、同様の処理を繰り返す。

【0077】また、ステップS37において、再生対象のコンテンツを、すべて再生したと判定された場合、処理を終了する。

【0078】以上のように、DVD-RAM36は、図3のDVDプレーヤと同一構成の図9のDVDプレーヤによって再生することができる。

【0079】なお、DVDレコーダのマスタキー記憶部41や、DVDプレーヤのマスタキー記憶部51に記憶されているマスタキーが、違法なコピーを行おうとする者（以下、適宜、違法者という）によって入手され、ライセンス契約を受けずに、図9（あるいは図3）に示したDVDプレーヤと同一構成のDVDプレーヤが製造されると、違法なコピーを行うことが可能となる。しかしながら、この場合、図4の鍵管理センタ31において、違法者が入手したマスタキーでディスクキーを暗号化した暗号化ディスクキー（以下、違法ディスクキーという）を、DVD-RAM36に記録する暗号化ディスクキーのセットから削除する（例えば、違法ディスクキーを、暗号化ディスクキーとしては用いられないオール0とする）ことにより、違法者によって入手されたマスタキーを有するDVDプレーヤにおけるDVD-RAM36の再生を不可能にすることができ、これにより、違法者による違法なコピーによる被害の拡大を防止することができる。

【0080】但し、この場合、違法者によって入手された違法ディスクキーが割り当てられていたメカには、新たなディスクキー（まだ、メカに割り当てられていないディスクキーのうちの1つ）を割り当てる必要がある。

【0081】次に、図7のDVDレコーダにおいては、DVD-RAM36に記録された暗号化ディスクキーを復号して得たディスクキーを利用して、コンテンツを暗号化し、DVD-RAM36に記録するようにしたが、暗号化したコンテンツは、DVD-RAM36に記録する他、伝送路を介して、遠方の装置（例えば、DVDプレーヤ）に伝送（提供）するようにすることも可能である。

【0082】図11は、そのようなDVDレコーダの構成例を示している。なお、図中、図7における場合と対応する部分については、同一の符号を付してある。即ち、図11のDVDレコーダは、図7における場合と基本的に同様に構成されている。

【0083】図11のDVDレコーダでは、図12のフローチャートに示すように、まず最初に、復号器42は、ステップS41において、DVD-RAM36のリードイン領域に記録された暗号化ディスクキーのセットの中から、割り当てマスタキーで暗号化されたものを読み出し、ステップS42に進み、マスタキー記憶部41に記憶されているマスタキーで復号して、ディスクキーを得る。このディスクキーは、復号部42から暗号化器43に供給される。

【0084】そして、ステップS43に進み、タイトルキー生成部44において、タイトルキーが生成され、暗号化器43に供給される。暗号化器43は、ステップS44において、タイトルキー生成部44から供給されるタイトルキーを、復号器42から供給されるディスクキーで暗号化する。さらに、ステップS44では、暗号化器43による結果得られる暗号化タイトルキーが、ステップS41でDVD-RAM36から読み出された暗号化ディスクキーのセットとともに、伝送路を介して伝送（提供）される。

【0085】その後、伝送すべきコンテンツが、暗号化器45に入力されると、暗号化器45は、ステップS45において、そのコンテンツを受信し、ステップS46に進み、そのコンテンツを、タイトルキー生成部44からのタイトルキーで暗号化し、伝送路を介して伝送する。そして、ステップS47に進み、伝送対象のコンテンツを、すべて伝送したかどうか判定され、まだ伝送していないと判定された場合、暗号化器45に、次のコンテンツが入力されるのを待って、ステップS45に戻り、以下、同様の処理を繰り返す。

【0086】また、ステップS47において、伝送対象のコンテンツを、すべて伝送したと判定された場合、処理を終了する。

【0087】以上のようにして伝送される暗号化ディスクキーのセット、暗号化タイトルキー、および暗号化コンテンツを受信した受信側では、図9に示したDVDプレーヤによって、コンテンツを再生することができる。

【0088】即ち、この場合、図9のDVDプレーヤで

は、図13のフローチャートに示すように、まず最初に、ステップS51において、伝送路を介して伝送されてくる、暗号化ディスクキーのセットが受信され、ステップS52に進み、復号器52は、その暗号化ディスクキーのセットの中から、マスターキー記憶部51に記憶されている割り当てマスターキーで暗号化されているものを抽出する。さらに、復号器52は、ステップS52において、マスターキー記憶部51に記憶されている割り当てマスターキーを読み出し、暗号化ディスクキーのセットの中から抽出した暗号化ディスクキーを、割り当てマスターキーで復号する。そして、復号器52は、その復号の結果得られるディスクキーを、復号器53に供給する。

【0089】復号器53は、ステップS53において、伝送路を介して伝送されてくる暗号化タイトルキーを受信し、ステップS54に進み、その暗号化タイトルキーを、復号器52からのディスクキーで復号する。そして、復号器53は、その復号の結果得られるタイトルキーを、復号器54に供給する。

【0090】復号器54は、ステップS55において、伝送路を介して伝送されてくる暗号化コンテンツを受信し、ステップS56に進み、その暗号化コンテンツを、復号器53からのタイトルキーで復号する。復号器54による復号の結果得られるデジタルデータのコンテンツは、A/D(Analog/Digital)変換され、アナログ信号とされて、外部に出力される。

【0091】そして、ステップS57に進み、受信対象のコンテンツを、すべて受信したかどうか判定され、まだ受信していないと判定された場合、ステップS55に戻り、次に伝送されてくる暗号化コンテンツが受信され、以下、同様の処理が繰り返される。

【0092】また、ステップS57において、受信対象のコンテンツを、すべて受信したと判定された場合、処理を終了する。

【0093】なお、上述の場合には、DVDデコーダからDVDプレーヤに対して、暗号化ディスクキーのセット、暗号化タイトルキー、および暗号化コンテンツを伝送するようにしたが、DVDレコーダからDVDプレーヤに対しては、暗号化タイトルキーと暗号化コンテンツを伝送し、DVDプレーヤにおいて、その割り当てマスターキーで暗号化された暗号化ディスクキーを、鍵管理センタ31から取得して、コンテンツを再生するようにすることも可能である。

【0094】次に、暗号化ディスクキーのセットは、DVD-RAM36に記録しておくのではなく、例えば、鍵管理センタ31などから、伝送路を介して、DVDレコーダに伝送し、DVDレコーダでは、伝送路を介して伝送されてくる暗号化ディスクキーのセットを受信し（取得し）、これを利用して、コンテンツを暗号化して、DVD-RAM36に記録することで、DVD-ROM10と同一フォーマットのDVD-RAM36を作

成するようにすることが可能である。

【0095】図14は、そのようなDVDレコーダの構成例を示している。なお、図中、図7における場合と対応する部分については、同一の符号を付してある。即ち、図14のDVDレコーダは、図7における場合と基本的に同様に構成されている。

【0096】図14のDVDレコーダでは、図15のフローチャートに示すように、まず最初に、ステップS61において、復号器42は、伝送路を介して伝送されてくる暗号化ディスクキーのセットを受信し、ステップS62に進む。ステップS62では、復号器42で受信された暗号化ディスクキーのセットが、DVD-RAM36のリードイン領域に記録され、ステップS63に進む。

【0097】ステップS63では、復号器42は、ステップS61で受信した暗号化ディスクキーの中から、割り当てマスターキーで暗号化されたものを抽出し、マスターキー記憶部41に記憶されている割り当てマスターキーで復号して、ディスクキーを得る。このディスクキーは、復号部42から暗号化器43に供給される。

【0098】そして、ステップS64に進み、以下、ステップS64乃至S68において、図8のステップS23乃至S27における場合とそれぞれ同様の処理が行われ、処理を終了する。

【0099】以上の処理により、図14のDVDレコーダにおいても、図9のDVDプレーヤで再生可能なDVD-RAM36を得ることができる。

【0100】即ち、図14のDVDレコーダによってコンテンツが記録されたDVD-RAM36は、図9に示したDVDプレーヤにおいて、図10のフローチャートにしたがった処理が行われることにより再生することができる。

【0101】次に、暗号化ディスクキーのセットは、例えば、鍵管理センタ31などから、伝送路を介して、DVDレコーダに伝送し、DVDレコーダでは、伝送路を介して伝送されてくる暗号化ディスクキーのセットを受信し（取得し）、これを利用して、コンテンツを暗号化し、さらに、その結果得られる暗号化コンテンツを、伝送路を介して、例えば、DVDプレーヤなどの遠方の装置に伝送（提供）するようにすることも可能である。

【0102】図16は、そのようなDVDレコーダの構成例を示している。なお、図中、図7における場合と対応する部分については、同一の符号を付してある。即ち、図16のDVDレコーダは、図7における場合と基本的に同様に構成されている。

【0103】図16のDVDレコーダでは、図17のフローチャートに示すように、まず最初に、ステップS71において、復号器42は、伝送路を介して伝送されてくる暗号化ディスクキーのセットを受信し、ステップS72に進む。ステップS72では、復号器42で受信さ

れた暗号化ディスクキーのセットが、伝送路を介して伝送され、ステップS73に進む。

【0104】ステップS73では、復号器42は、ステップS71で受信した暗号化ディスクキーの中から、割り当てマスターキーで暗号化されたものを抽出し、マスターキー記憶部41に記憶されているマスターキーで復号して、ディスクキーを得る。このディスクキーは、復号部42から暗号化器43に供給される。

【0105】そして、ステップS74に進み、タイトルキー生成部44において、タイトルキーが生成され、暗号化器43に供給される。暗号化器43は、ステップS75において、タイトルキー生成部44から供給されるタイトルキーを、復号器42から供給されるディスクキーで暗号化し、その結果得られる暗号化タイトルキーを、伝送路を介して伝送（提供）する。

【0106】その後、ステップS76に進み、以下、ステップS76乃至S78において、図12のステップS45乃至S47における場合とそれぞれ同様の処理が行われ、処理を終了する。

【0107】以上のようにして伝送される暗号化ディスクキーのセット、暗号化タイトルキー、および暗号化コンテンツを受信した受信側では、図9に示したDVDプレーヤによって、図13のフローチャートにしたがった処理が行われることにより、コンテンツを再生することができる。

【0108】次に、DVDプレーヤにおいて、暗号化ディスクキーのセットを、DVDレコーダに提供し、DVDレコーダにおいて、その暗号化ディスクキーのセットを利用して、コンテンツを暗号化し、DVDプレーヤに提供して、DVDプレーヤでは、DVDレコーダに提供した暗号化ディスクキーのセットを利用して、DVDレコーダから提供される暗号化コンテンツを再生することが可能である。

【0109】図18は、そのようなDVDレコーダとDVDプレーヤからなるDVDシステムの構成例を示している。

【0110】図18のDVDシステムは、DVDレコーダ61とDVDプレーヤ62とから構成されており、DVDレコーダ61は、図16に示したように構成され、そこでは、図17のフローチャートにしたがった処理が行われる。

【0111】一方、DVDプレーヤ62は、例えば、図9に示したように構成され、そこでは、図19に示すフローチャートにしたがった処理が行われる。

【0112】即ち、DVDプレーヤ62では、まず最初に、ステップS81において、例えば、DVD-RAM36に記録された暗号化ディスクキーのセットが読み出され、あるいは、鍵管理センタ31などから伝送路を介して伝送されてくる暗号化ディスクキーのセットが受信され、その暗号化ディスクキーのセットが、伝送路を介

して、DVDレコーダ61に伝送される。

【0113】そして、ステップS82に進み、復号器52は、DVDレコーダ61に伝送された暗号化ディスクキーのセットの中から、マスターキー記憶部51に記憶されている割り当てマスターキーで暗号化されているものを抽出する。さらに、復号器52は、ステップS82において、マスターキー記憶部51に記憶されている割り当てマスターキーを読み出し、暗号化ディスクキーのセットの中から抽出した暗号化ディスクキーを、割り当てマスターキーで復号する。そして、復号器52は、その復号の結果得られるディスクキーを、復号器53に供給する。

【0114】復号器53は、ステップS83において、DVDレコーダ61から、伝送路を介して伝送されてくる暗号化タイトルキーを受信し、ステップS84に進み、その暗号化タイトルキーを、復号器52からのディスクキーで復号する。そして、復号器53は、その復号の結果得られるタイトルキーを、復号器54に供給する。

【0115】復号器54は、ステップS85において、DVDレコーダ61から、伝送路を介して伝送されてくる暗号化コンテンツを受信し、ステップS86に進み、その暗号化コンテンツを、復号器53からのタイトルキーで復号する。復号器54による復号の結果得られるデジタルデータのコンテンツは、A/D(Analog/Digital)変換され、アナログ信号とされて、外部に出力される。

【0116】そして、ステップS87に進み、受信対象のコンテンツを、すべて受信したかどうかが判定され、まだ受信していないと判定された場合、ステップS85に戻り、DVDレコーダ61から、次に伝送されてくる暗号化コンテンツを受信し、以下、同様の処理を繰り返す。

【0117】また、ステップS87において、受信対象のコンテンツを、すべて受信したと判定された場合、処理を終了する。

【0118】次に、上述した一連の処理は、ハードウェアにより行うこともできるし、ソフトウェアにより行うこともできる。一連の処理をソフトウェアによって行う場合には、そのソフトウェアを構成するプログラムが、専用のハードウェアとしてのDVDレコーダやDVDプレーヤに組み込まれているコンピュータや、汎用のコンピュータ等にインストールされる。

【0119】そこで、図20を参照して、上述した一連の処理を実行するプログラムをコンピュータにインストールし、コンピュータによって実行可能な状態とするために用いられる、そのプログラムが記録されているプログラム記録媒体について説明する。

【0120】プログラムは、図20(A)に示すように、コンピュータ101に内蔵されている記録媒体としてのハードディスク102や半導体メモリ103に予め

記録しておくことができる。

【0121】あるいはまた、プログラムは、図20(B)に示すように、フロッピー（登録商標）ディスク111、CD-ROM(Compact Disc Read Only Memory)112、MO(Magneto optical)ディスク113、DVD(Digital Versatile Disc)114、磁気ディスク115、半導体メモリ116などの記録媒体に、一時的あるいは永続的に格納（記録）しておくことができる。このような記録媒体は、いわゆるパッケージソフトウェアとして提供することができる。

【0122】なお、プログラムは、上述したような記録媒体からコンピュータにインストールする他、図20(C)に示すように、ダウンロードサイト121から、デジタル衛星放送用の人工衛星122を介して、コンピュータ101に無線で転送したり、LAN(Local Area Network)、インターネットといったネットワーク131を介して、コンピュータ123に有線で転送し、コンピュータ101において、内蔵するハードディスク102などにインストールすることができる。

【0123】また、本明細書において、コンピュータに各種の処理を行わせるためのプログラムを記述する処理ステップは、必ずしもフローチャートとして記載された順序に沿って時系列に処理する必要はなく、並列的あるいは個別に実行される処理（例えば、並列処理あるいはオブジェクトによる処理）も含むものである。

【0124】次に、図21は、図20のコンピュータ101の構成例を示している。

【0125】コンピュータ101は、図21に示すように、CPU(Central Processing Unit)142を内蔵している。CPU142には、バス141を介して、入出力インタフェース145が接続されており、CPU142は、入出力インタフェース145を介して、ユーザによって、キーボードやマウス等で構成される入力部147が操作されることにより指令が入力されると、それにしたがって、図20(A)の半導体メモリ103に対応するROM(Read Only Memory)143に格納されているプログラムを実行する。あるいは、また、CPU142は、ハードディスク102に格納されているプログラム、衛星122若しくはネットワーク131から転送され、通信部148で受信されてハードディスク102にインストールされたプログラム、またはドライブ149に装着されたフロッピーディスク111、CD-ROM112、MOディスク113、DVD114、若しくは磁気ディスク115から読み出されてハードディスク102にインストールされたプログラムを、RAM(Random Access Memory)144にロードして実行する。そして、CPU142は、その処理結果を、例えば、入出力インタフェース145を介して、LCD(Liquid Crystal Display)等で構成される表示部146に、必要に応じて出力する。

【0126】なお、本実施の形態では、RAMメディア

として、DVD-RAMを用いた場合について説明したが、本発明は、DVD-RAM以外の光ディスク、光磁気ディスク、磁気ディスク、磁気テープ等のRAMメディアにも適用可能である。

【0127】さらに、本実施の形態では、ディスクキーで暗号化されるタイトルキーで、コンテンツを暗号化するようにしたが、コンテンツの暗号化は、タイトルキーを用いずに、ディスクキーで行うようにすることも可能である。

10 【0128】また、DVD-RAM36には、画像や音声のデータその他、コンピュータによって実行されるプログラム等を記録することが可能である。

【0129】

【発明の効果】本発明のデータ提供装置およびデータ提供方法、並びにプログラム記録媒体によれば、第1キーで暗号化された第2キーである暗号化第2キーが取得され、暗号化第2キーが、第1キーに基づいて復号される。そして、その復号された第2キーを利用して、データが暗号化され、その暗号化されたデータである暗号化

20 データが提供される。従って、第1キーで暗号化される第2キーを利用して暗号化したデータを得ることができる。

【0130】本発明のデータ記録媒体によれば、第1キーで暗号化された第2キーである暗号化第2キーが記録されており、後に、暗号化第2キーが、第1キーで復号され、その結果得られる第2キーを利用して、データが暗号化されて記録される。従って、第1キーで暗号化される第2キーを利用して暗号化したデータを記録することができる。

30 【0131】本発明のデータ記録媒体の製造方法によれば、後に、第1キーで暗号化された第2キーである暗号化第2キーを、第1キーで復号し、第2キーを得て、その第2キーを利用して、データが暗号化されて記録されるデータ記録媒体に、暗号化第2キーが記録される。従って、第1キーで暗号化される第2キーを利用して暗号化したデータを記録することのできるデータ記録媒体を製造することができる。

【図面の簡単な説明】

40 【図1】DVD-ROMの製造工程を説明するための図である。

【図2】DVD規格のディスクフォーマットを示す図である。

【図3】従来のDVDプレーヤの一例の構成例を示すブロック図である。

【図4】本発明を適用したDVD-RAMの製造工程を説明するための図である。

【図5】図4の鍵管理センタ31における処理を説明するためのフローチャートである。

50 【図6】図4のディスク製造業者33における処理を説明するためのフローチャートである。

21

【図 7】本発明を適用したDVDレコーダの第1実施の形態の構成例を示すブロック図である。

【図 8】図 7 のDVDレコーダの処理を説明するためのフローチャートである。

【図 9】コンテンツを再生するDVDプレーヤの構成例を示すブロック図である。

【図 10】図 7 のDVDレコーダによってコンテンツが記録されたDVD-RAMを再生する場合の、図 9 のDVDプレーヤの処理を説明するためのフローチャートである。

【図 11】本発明を適用したDVDレコーダの第2実施の形態の構成例を示すブロック図である。

【図 12】図 11 のDVDレコーダの処理を説明するためのフローチャートである。

【図 13】図 11 のDVDレコーダから送信されてくるコンテンツを再生する場合の、図 9 のDVDプレーヤの処理を説明するためのフローチャートである。

【図 14】本発明を適用したDVDレコーダの第3実施の形態の構成例を示すブロック図である。

【図 15】図 14 のDVDレコーダの処理を説明するためのフローチャートである。

【図 16】本発明を適用したDVDレコーダの第4実施の形態の構成例を示すブロック図である。

【図 17】図 16 のDVDレコーダの処理を説明するためのフローチャートである。

22

【図 18】本発明を適用したDVDシステムの一実施の形態の構成例を示すブロック図である。

【図 19】図 18 のDVDプレーヤ 62 の処理を説明するためのフローチャートである。

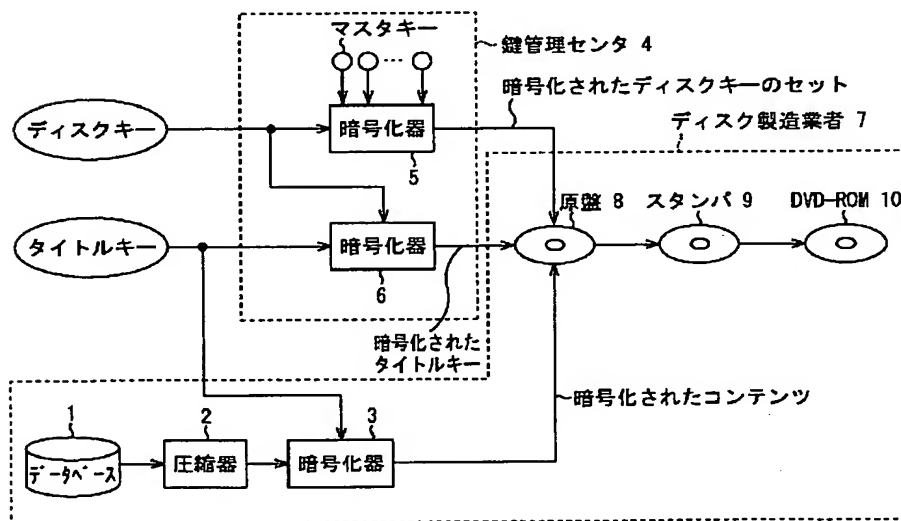
【図 20】本発明を適用したプログラム記録媒体を説明するための図である。

【図 21】図 20 のコンピュータ 101 の構成例を示すブロック図である。

#### 【符号の説明】

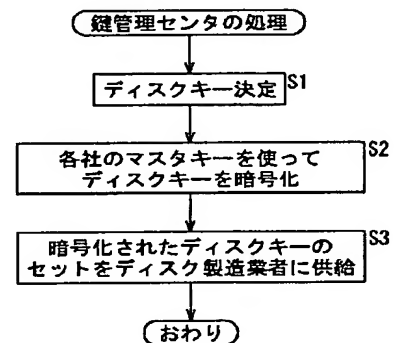
- 10 31 鍵管理センタ, 32 暗号化器, 33 ディスク製造業者, 34 原盤, 35 スタンパ, 36 DVD-RAM, 41 マスタキー記憶部, 42 復号器, 43 暗号化器, 44 タイトルキー生成部, 45 暗号化器, 51 マスタキー記憶部, 52 乃至 54 復号器, 61 DVDレコーダ, 62 DVDプレーヤ, 101 コンピュータ, 102 ハードディスク, 103 半導体メモリ, 111 フロッピーディスク, 112 CD-ROM, 113 MOディスク, 114 DVD, 115 磁気ディスク, 116 半導体メモリ, 121 ダウンロードサイト, 122 衛星, 131 ネットワーク, 141 バス, 142 CPU, 143 ROM, 144 RAM, 145 入出力インタフェース, 146 表示部, 147 入力部, 148 通信部, 149 ドライブ

【図 1】

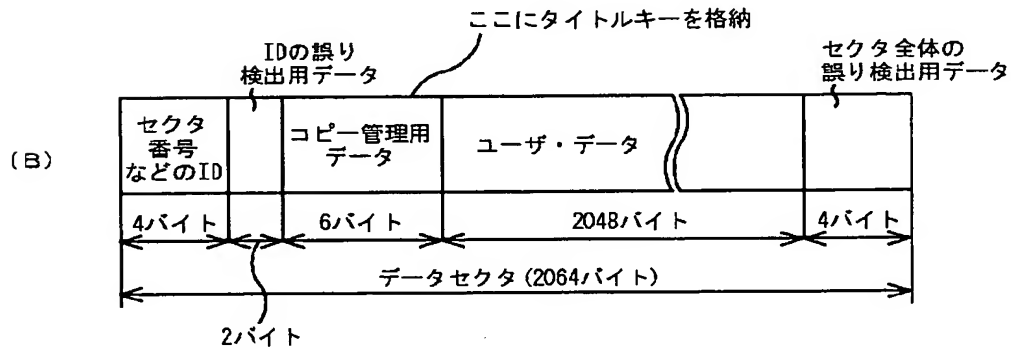
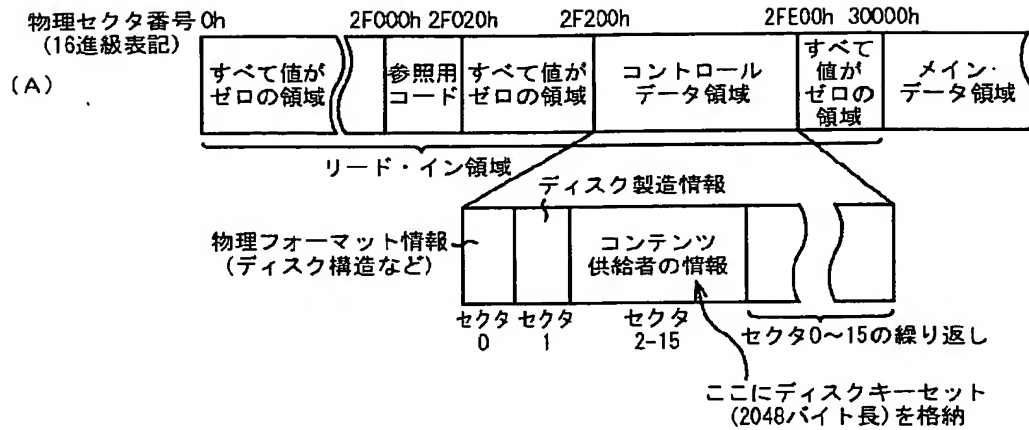


DVD-ROMの製造工程

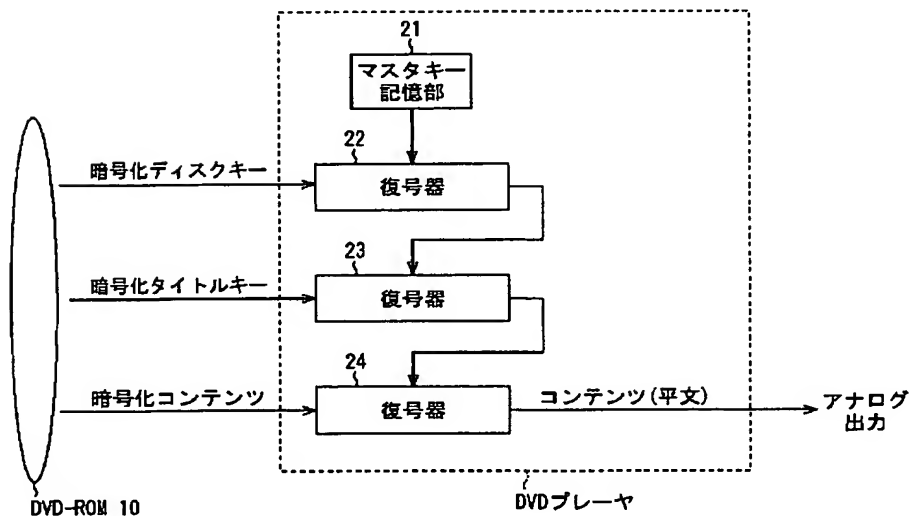
【図 5】



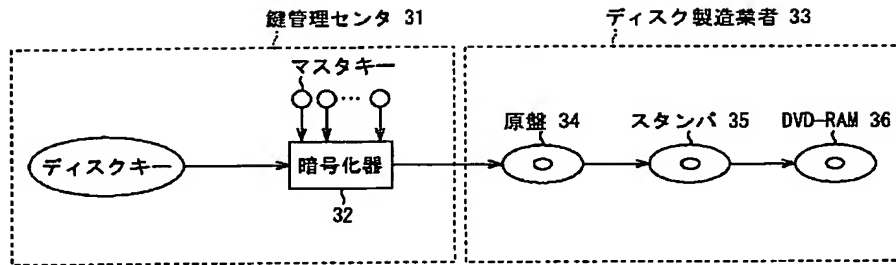
【図2】



【図3】

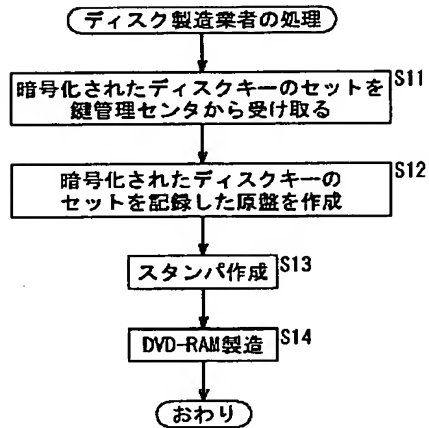


【図4】

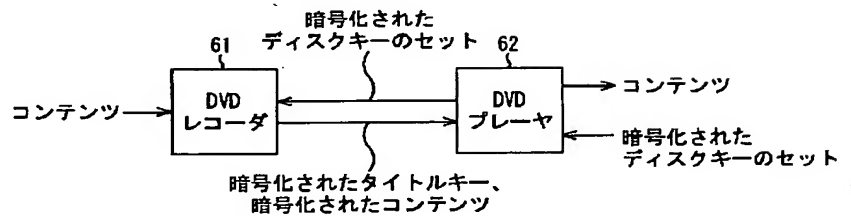


## DVD-RAMの製造工程

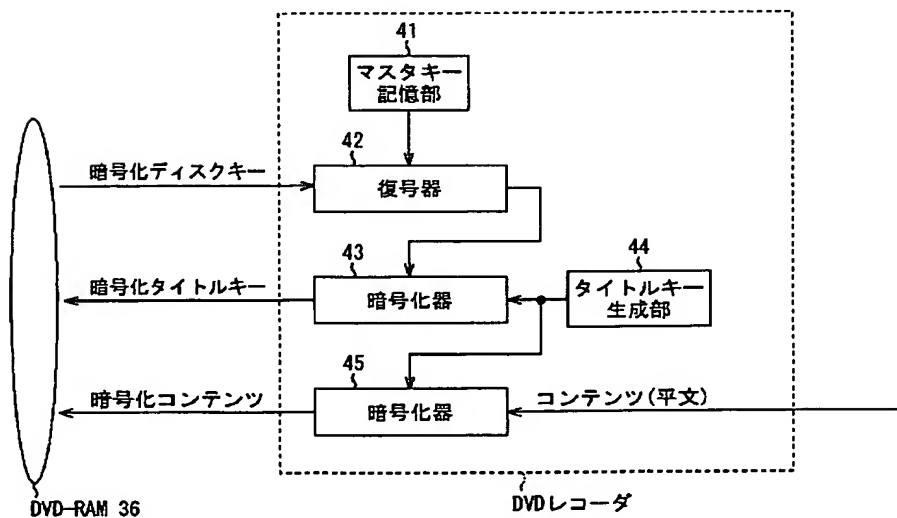
【図6】



【図18】

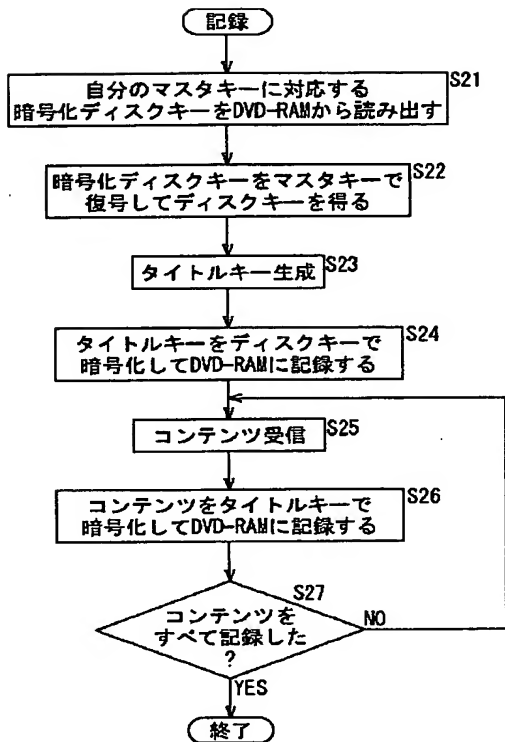


【図7】

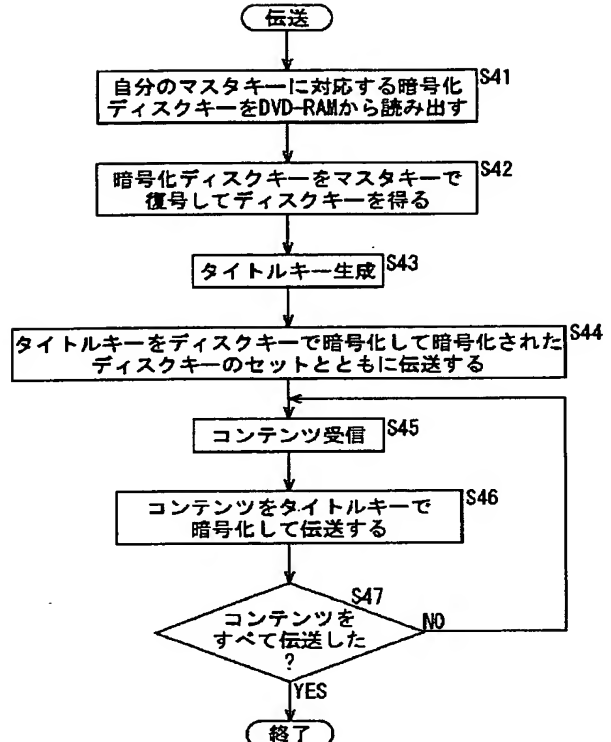




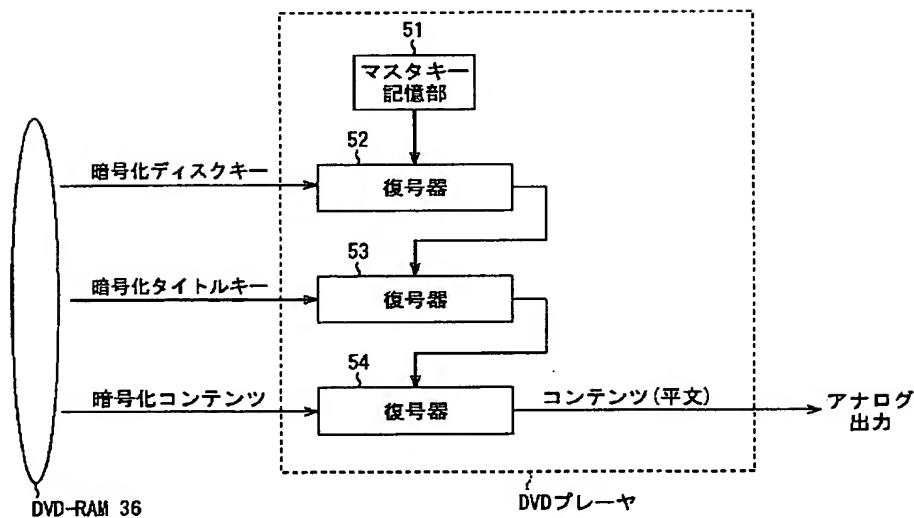
【図8】



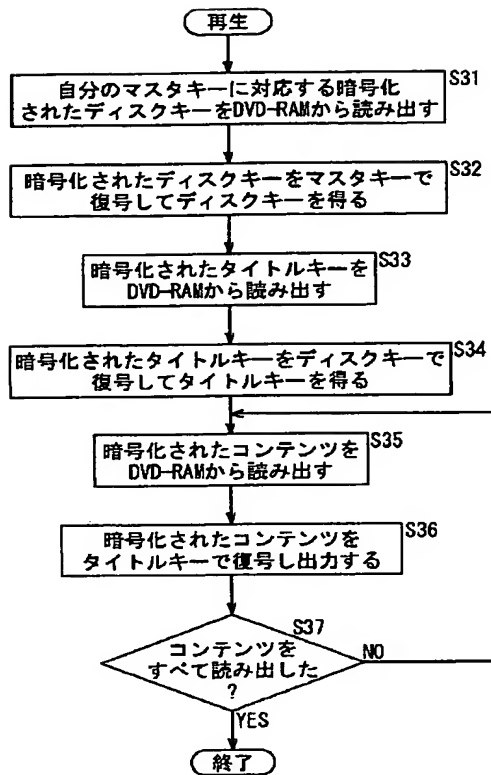
【図12】



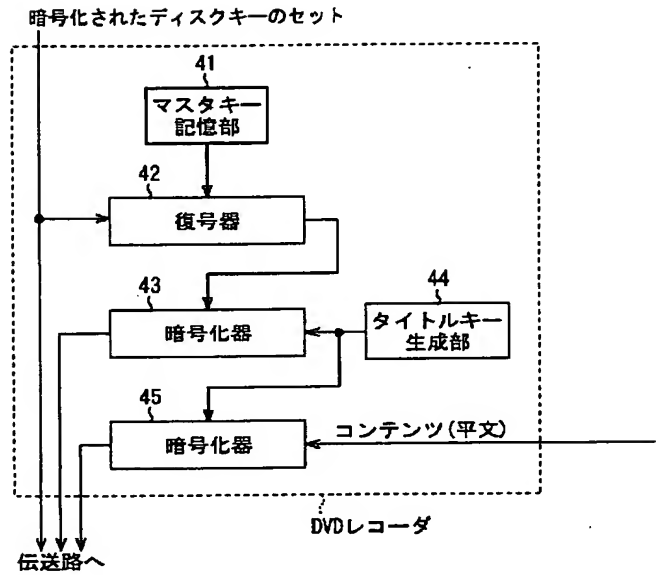
【図9】



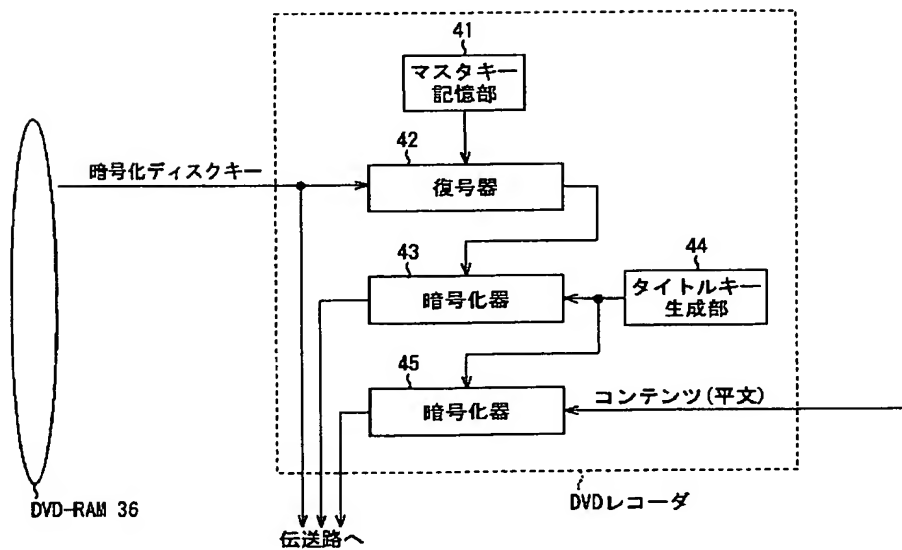
【図10】



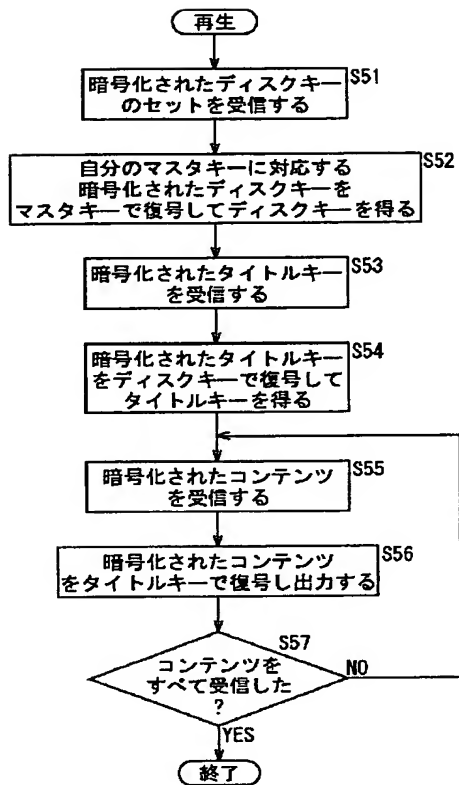
【図16】



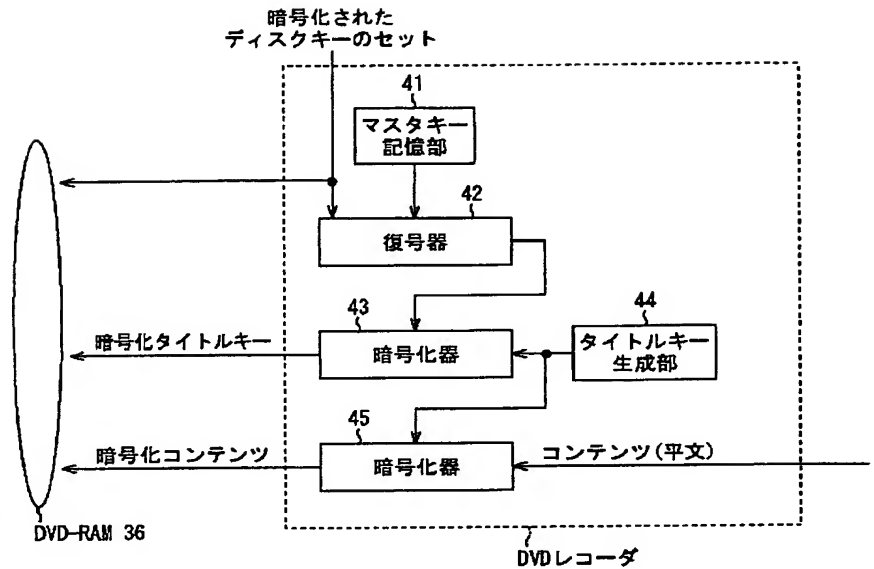
【図11】



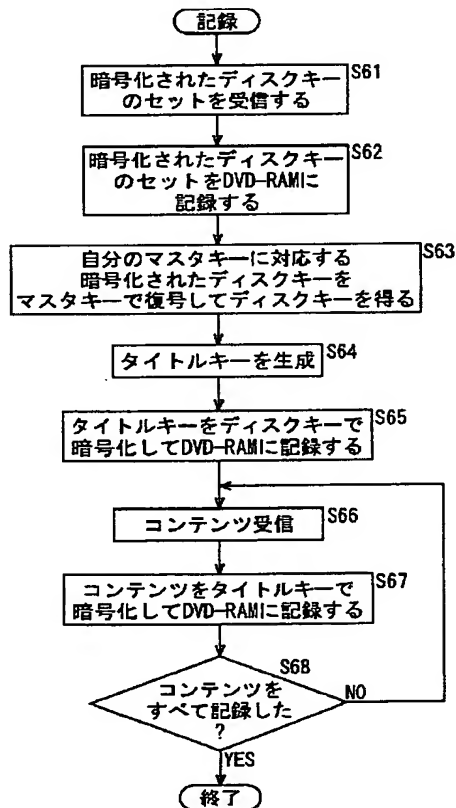
【図13】



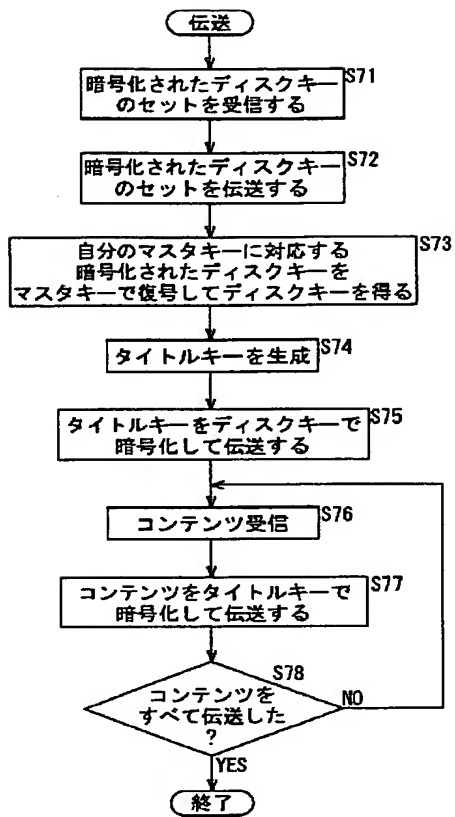
【図14】



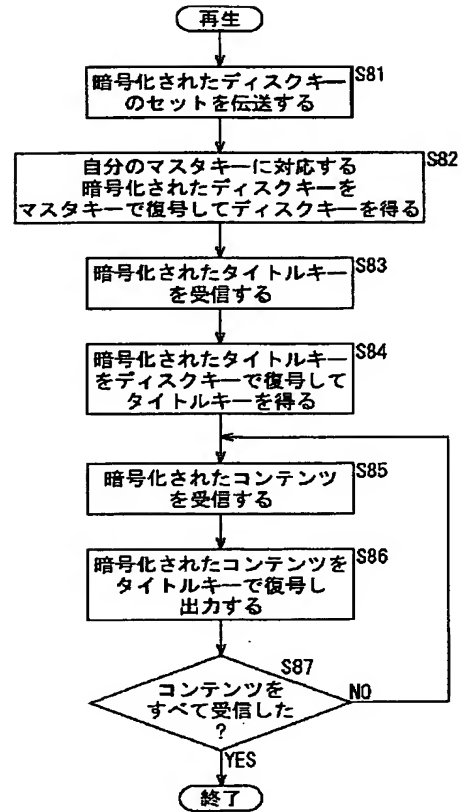
【図15】



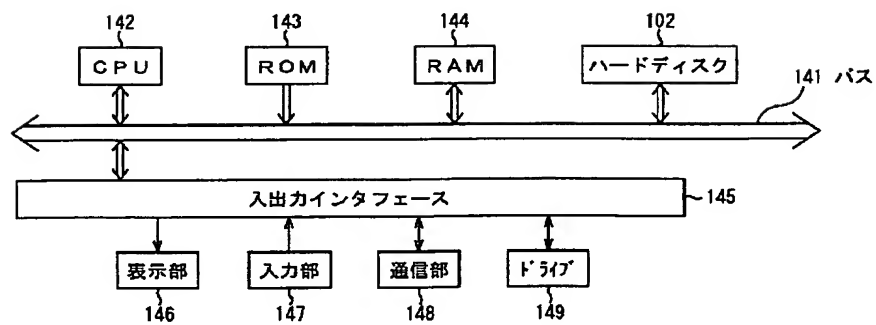
【図17】



【図19】

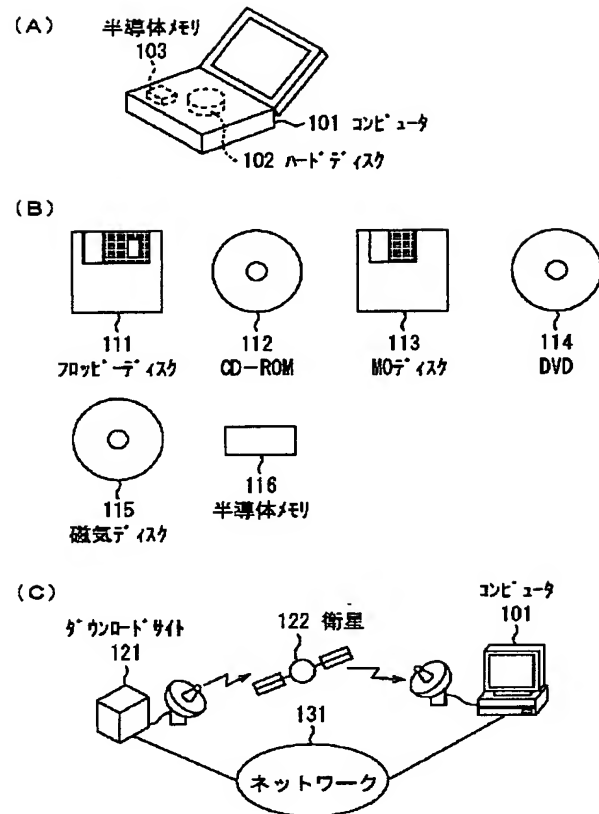


【図21】



コンピュータ 101

【図 20】



フロントページの続き

(51) Int. Cl.<sup>7</sup>  
H 0 4 N 5/91

識別記号

F I  
H 0 4 L 9/00  
H 0 4 N 5/91

テーマコード(参考)

6 0 1 E  
P

Fターム(参考) 5B017 AA06 BA07 BB02 BB03 CA09  
CA16  
5C052 AA04 AB03 AB05 CC11 DD04  
5C053 FA13 FA25 GA11 GB06 GB21  
GB38 JA03  
5D044 BC03 CC04 DE49 DE50 EF05  
FG18 GK17 HL08 HL11  
5J104 AA01 AA12 AA16 EA04 EA06  
EA08 EA18 EA22 JA03 NA02  
NA03 NA32 PA00 PA14